Fall 2022, Math 522: Week 12 Problem Set
Due: Friday, December 2nd, 2022
Quadratic Residues

Discussion problems. The problems below should be worked on in class.

(D1) *Using the reciprocity law.* Recall that for distinct primes p and q, we have

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless $p \equiv q \equiv 3 \bmod 4$, in which case $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(a) Using the piecewise formula for $\left(\frac{2}{p}\right)$ from class, prove that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

(b) Find a formula for $\left(\frac{-1}{p}\right)$ in the spirit of part (a).

(c) Using the quadratic reciprocity law, prove

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

for any distinct odd primes p and q.

(D2) *Extending the use of Legendre symbols.* We will prove the following theorem.

Theorem. *If p is an odd prime and $p \nmid a$, then*

$$x^2 \equiv a \bmod p^k$$

has a solution if and only if $\left(\frac{a}{p}\right) = 1$.

(a) Use the above theorem to determine if $x^2 \equiv 22 \bmod 81$ has a solution.

(b) Argue that if $x^2 \equiv a \bmod p^k$, then $x^2 \equiv a \bmod p$. Conclude the forward direction.

(c) For the backward direction, we proceed by induction on k. Prove the base case $k = 1$.

(d) Now, assume $x^2 \equiv a \bmod p^k$ (the inductive hypothesis). Argue that there exist $y, m, r \in \mathbb{Z}$ such that $x^2 = a + mp^k$ and $xy = 1 + rp$.

(e) Argue that $(x - \frac{1}{2}my(p+1)p^k)^2 \equiv a \bmod p^{k+1}$.
Hint: start with the left hand side, distribute, and simplify (modulo p^{k+1}) until the right hand side is obtained.
This part requires several steps of algebra, so plan your boardspace accordingly.

(f) Conclude the theorem holds.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Determine whether 70 is a quadratic residue modulo 101 without using a calculator.
Hint: use the property $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ of Legendre symbols and the quadratic reciprocity law to your advantage to compute $\left(\frac{70}{101}\right)$.

(H2) Determine whether 1823 is a quadratic residue modulo 83521 without using a calculator.
Hint: $83521 = 17^4$.

(H3) Prove that if p is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11 \bmod 12; \\ -1 & \text{if } p \equiv 5, 7 \bmod 12. \end{cases}$$

(H4) Determine whether each of the following is true or false. Prove each true statement, and give a counterexample for each false statement.

(a) Given a and n with $n \geq 2$, the equation

$$x^2 \equiv a \bmod n$$

has at most 2 incongruent solutions for x modulo n.

(b) If p and q are odd primes and $\gcd(a, pq) = 1$, then

$$x^2 \equiv a \bmod pq$$

has a solution if and only if $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{q}\right) = 1$